Design of Navigation Message Authentication Assisted by Ground Based Augmentation Systems

Muzi Yuan, Zhe Liu, Xiaomei Tang, Shengqiang Lou and Gang Ou

Abstract Spoofing attack organized by generating fake navigation signal can precisely manipulate PNT output of target receiver. In this paper an authenticated augmentation message for GBAS is designed to obtain the authentication for both navigation message from satellites and augmentation message from GBAS broadcasters. The proposed navigation message authentication method has an advantage in efficiency and authentication delay compared with legacy schemes integrated into satellite signal while has an equally high security level as other schemes.

Keywords Anti-spoofing · Ground based augmentation system
Navigation message authentication

1 Introduction

While an increasing number of critical infrastructures rely on the integrity of GNSS service, life security may be threatened by spoofing attacks [1]. GNSS spoofing attack refers to the attack performed by broadcasting a counterfeit GNSS signal to the target receiver. Receivers cannot distinguish an authorized signal from its fake replica without extra information. Navigation message authentication (NMA) is an effective method to verify the integrity of navigation message by signature or other message authentication codes (MACs).

A number of NMA methods integrated in satellite signal has been proposed in recent years [2–7]. The efficiency of these methods are measured by time to first authenticated fix (TTFAF) and time between authentications (TBA) [8]. In latest research, NMA based on satellite signal can achieve a TTFAF and TBA of 10 s in Galileo open service [6]. Main drawbacks of these NMA methods is the relatively

M. Yuan · Z. Liu · X. Tang · S. Lou · G. Ou (✉)
School of Electronic Science, National University of Defense Technology, 410073 Changsha, China
e-mail: ougangcs@139.com

J. Sun et al. (eds.), *China Satellite Navigation Conference (CSNC) 2018 Proceedings*, Lecture Notes in Electrical Engineering 497,
https://doi.org/10.1007/978-981-13-0005-9_64

low bitrate and the weak adjustability of navigation message in satellite signal. Low bitrate requires long transition time and weak adjustability leads to huge amount of bits involved in a single NMA fix.

Signal of ground based augmentation system (GBAS) has the advantage of higher bitrate and more agile message arrangement compared with satellite signal. There are many methods raised for GBAS to improve the performance of GNSS [9–11]. However, there are few literature focusing on the possibility of implementing an NMA assisted by GBAS broadcasters. We proposed a basic design of NMA assisted by GBAS broadcasters to obtain a high efficiency and a high robustness against spoofing attacks.

The paper is organized as follows: the principle and model of NMA protection against spoofing attack are discussed in Sect. 2; the proposed implementation of NMA assisted by GBAS is demonstrated in Sect. 3; an analysis of performance is performed in Sect. 4.

2 Model of NMA Protection Against Spoofing Attack

Spoofing attacks neutralized by NMA are categorized as intermediate spoofing attack and estimation and replay attack [12]. The first category is performed by generating counterfeit GNSS signal based on the real position and the spoofing position of target and estimating the navigation message for spoofing attack. The second category is performed by recording and tampering the authorized GNSS signal and replaying it in spoofing scenarios. NMA is able to protect the integrity of GNSS service against spoofing attack by recognizing those falsify in navigation message. In this chapter model of spoofing attack and NMA are discussed.

2.1 Model of Spoofing Attacks

Receivers perform a position, velocity and time (PVT) solution by implying parameters (x_i, y_i, z_i, ρ_i) form GNSS signal into Eq. (2.1).

$$\sqrt{(x_i - x_r)^2 + (y_i - y_r)^2 + (z_i - z_r)^2} + c\Delta t_{r-s} = \rho_i, i = 1, \ldots, N \tag{2.1}$$

Here in Eq. (2.1) (x_i, y_i, z_i) and (x_r, y_r, z_r) are coordinate of satellite and receiver, c is the speed of light, Δt_{r-s} is the clock differential between receiver and satellite, ρ_i is the pseudorange measurement from satellite to receiver.

Since parameter (x_i, y_i, z_i) is determined by navigation message, spoofing attackers can generate fake navigation message to lead the receiver believe in spoofed parameter (x_i', y_i', z_i'). If the spoofed parameter (for example in satellite

No. 1) fulfills Eq. (2.2), the receiver will make a PVT solution $(x'_r, y'_r, z'_r, \Delta t'_{r-s})$ under the manipulation of spoofing attackers.

$$\begin{aligned}&\sqrt{(x'_1 - x'_r)^2 + (y'_1 + y'_r)^2 + (z'_1 + z'_r)^2} + c\Delta t'_{r-s} = \rho'_1\\&\sqrt{(x_i - x'_r)^2 + (y_i + y'_r)^2 + (z_i + z'_r)^2} + c\Delta t'_{r-s} = \rho_i, i = 2, \ldots, N\end{aligned} \tag{2.2}$$

Hence, the combination of authorized signal and spoofed signal can be modeled as Eq. (2.3).

$$Y_k = \alpha\hat{w}_{k-d}c_{k-d} + w_k c_k + N_k \tag{2.3}$$

Here in the model, $\hat{w}_{k-d}$ is the manipulated navigation message fulfills Eq. (2.2), c_{k-d} is the delayed pseudorange code, w_k and c_k are navigation message and pseudorange code broadcasted by authorized satellite. α is the energy gain of spoofing signal and N_k is noise.

2.2 Principle of Navigation Message Authentication

The basic function of NMA is to distinguish $\hat{w}_{k-d}$ from w_k in Eq. (2.3). Most NMA schemes are based on signature or MAC algorithms such as elliptic curve digital signature algorithm (ECDSA) [13] and timed efficient stream loss-tolerant authentication (TESLA) [14].

ECDSA uses key pairs to ensure message authentication. Private keys which are only held by satellites are employed to sign message while public keys which are published to public are employed to verify the signature attached to the message. TESLA uses key stream to derive MACs form message. Keys to verify MACs are announced after MACs are broadcasted to protect privacy.

In NMA schemes previously proposed the combination of NMA protected signal and spoofed signal can be modeled as Eq. (2.4).

$$Y_k = \alpha(\hat{w}_{k-d}||\hat{s}_{k-d})c_{k-d} + (w_k||s_k)c_k + N_k \tag{2.4}$$

Here in Eq. (2.4) operator $||$ is to merge to strings, s_k is signature or MAC derived by NMA schemes. Since spoofing attackers have no access to private keys or unannounced MAC keys, fake signature or MAC $\hat{s}_{k-d}$ will not pass any verification in receivers. Hence receivers can identify authorized signal under protection of NMA.

In the proposed scenario of this paper, receivers are under the coverage of GBAS broadcaster. Hence NMA messages are transmitted through GBAS signals. The structure of proposed NMA is shown in Fig. 1.

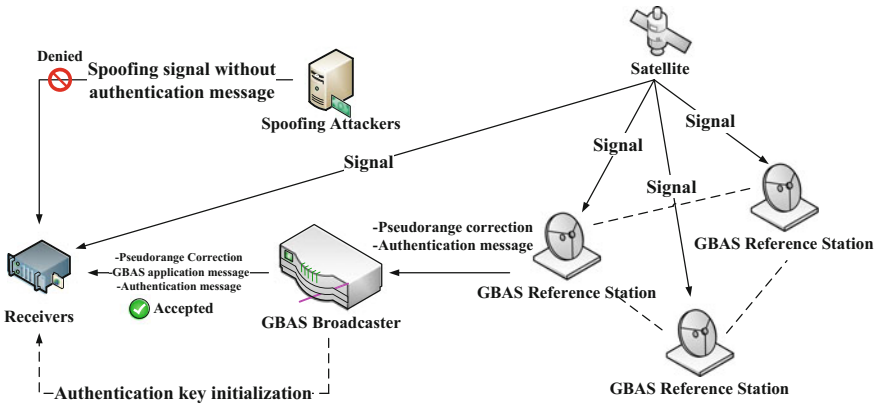

Fig. 1 The structure of proposed NMA

3 NMA Implementation with GBAS Broadcasters

While the NMA is integrated into satellite signal, those signatures or MACs are extra information of legacy navigation message which require modification in the navigation message and occupy extra communication bandwidth of satellites. The GBAS broadcaster can provide a data transmission rate up to 40.5 Kbps, which is much higher than the 50 bps (120 bps for Galileo) navigation message. If NMA is provided by third-party information source such as GBAS broadcasters the capacity and agility of authentication message may be extended.

In this chapter we propose an implementation of NMA scheme provided by GBAS broadcasters. The structure of broadcasting information are specified and the behaviour of both GBAS providers and receivers are described.

3.1 Structure of NMA Protected GBAS Broadcasting Message

In previously proposed GBAS implementations, broadcasting messages are composed of various message types including pseudorange corrections, ground based ranging source information and information for other applications [11]. The proposed NMA scheme is integrated into GBAS broadcasting by a new message type composed of three sections: frame information section, navigation message authentication section (NMAS) and GBAS message authentication section (GMAS).

The NMAS is the section to authenticate navigation message broadcasted by satellites. The NMAS is composed of frame ID, page ID, time information and authentication message. The authentication message is calculated via navigation

Table 1 Data structure of NMAS and GMAS for D1 navigation message in BeiDou system

Data content	Bits used	Range of values
Message type ID	8	0–255
PRN ID	6	0–63
Frame ID	3	1–5
Page ID	7	1–24
Time identifier	–	–
Week number	13	0–8191
Second of week	20	0–604,800
NMAS authentication message	Variable	–
GMAS authentication message	Variable	–

message of the particular frame and page indicated in the head of the NMAS. The GMAS is the section to authenticate the integrity of GBAS message itself. The GMAS is an authentication message for all the messages broadcasted in the interval of two frames.

As an example, the data structure of NMAS and GMAS for D1 navigation message in BeiDou system is shown in Table 1.

The NMAS and GMAS are broadcasted after every frame is delivered. This time interval is 6 s in D1 navigation message of BeiDou system. Message length of both NMAS and GMAS are variable for various security requirements. For critical scenarios, message length of NMA may achieve the maximum length of 569 bits.

3.2 Generation of NMAS and GMAS Messages

NMAS messages are generated through satellite signal after every frame is delivered. GBAS first check the integrity of navigation message by calculating and comparing the positioning solution with its real location. Then frame ID, page ID and time information are extracted from the navigation message. Authentication message of this frame is calculated and truncated via secure hash algorithms (for example SHA-256). The process of NMAS messages is shown in Fig. 2.

GMAS message is a signature of all the GBAS messages broadcasted in last interval of navigation message frame, which is generated through private keys and verified through public keys. GBAS calculate and truncate the signature via asymmetric cryptographic algorithms (for example ECDSA). The process of GMAS messages is shown in Fig. 3.

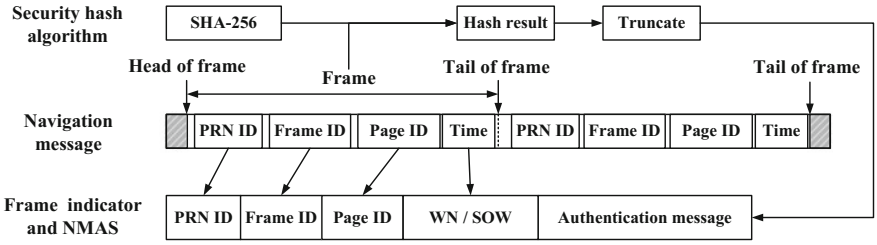

Fig. 2 Generation of frame indicator and NMAS from received navigation message

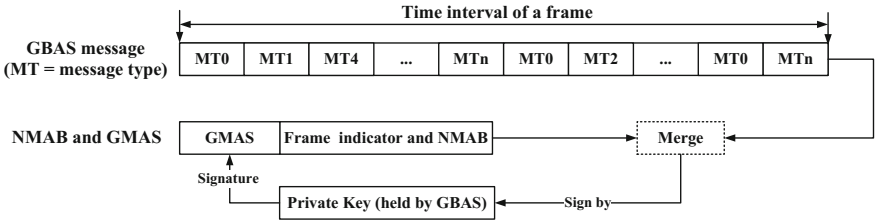

Fig. 3 Generation of GMAS from GBAS message and the form of NMA message type

3.3 Verification of NMAS and GMAS Messages

After receiving a whole frame of navigation message, receivers first verify the integrity of GBAS message by verifying if the signature in GMAS is consistent with GBAS message received in last frame interval. While GBAS message is reliable, receivers calculate hash result of the navigation message frame indicated in the frame information section via the same security hash algorithm. If the result matches with the NMAS, the navigation message frame will pass the authentication. Otherwise a bit error or spoofing attack can be detected.

Verification logic diagram is shown in Fig. 4.

In the proposed scheme, the GBAS augment message is easier to be authenticated than the navigation message. Thus the verification of GBAS augment message is set up before NMA to ensure security.

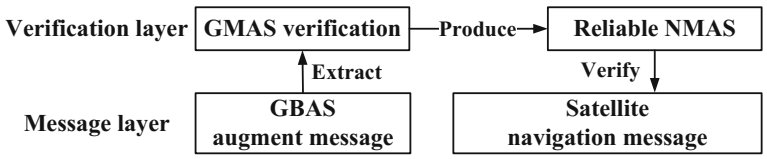

Fig. 4 Logic diagram of authentication verification

4 Performance Analysis

Performance of NMA can be indicated from the aspect of security and efficiency. For security indicators, this paper takes the average attack time (AAT) and the possibility of false alarm (PFA) into consideration. For efficiency indicators, the TTFAF and TBA are taken into consideration.

4.1 Security

The security of the proposed NMA scheme is ensured by secure hash algorithm and asymmetric cryptographic algorithm. Introduced in a 1998 report, it takes 3 months of a network of 50,000 Pentium Pro 200 MHz machines to crack a ECCp-109 challenge in ECDSA [13]. Based on Moore's law and analysis of hardware associate [15], the estimating time to crack a ECDSA signature system by the network of 50,000 mainstream machines can be shown as Table 2.

For a normal expiration period (e.g. 1 year), ECDSA is secure for NMA in predictable future.

4.2 Efficiency

The GBAS broadcasting data rate (40.5 Kbps) is much higher than civil navigation message (120 bps in Galileo and 50 bps in other systems). Hence a broadcast of 569 bit NMA message every frame only cost a minor partition of broadcasting ability and can be fulfilled easily.

In analysis below, we take D1 navigation message in BeiDou system as an example. While public keys have been initialled into receivers, mean TTFAF and TBA can be calculated via Eqs. (4.1) and (4.2).

$$\overline{TTFAF} = \frac{1}{L_f} \cdot \sum_{n=1}^{L_f} \frac{(n + L_f)T_b}{(1 - BER)^{L_f}} \tag{4.1}$$

Table 2 Crack time estimation for different length of key by different platforms

Key length	Pentium M	XC3S1000 [15]	ASIC
96	10 h	3.6 h	–
128	97 years	51 years	5 months
160	7.6×10^6 years	6.2×10^5 years	5.0×10^4 years
233 (estimate)	5.0×10^{16} years	4.1×10^{15} years	3.3×10^{14} years

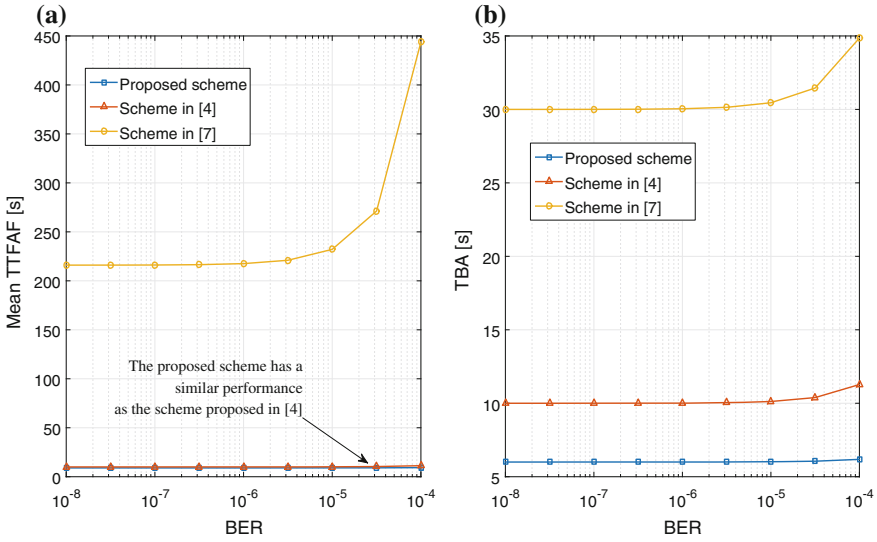

Fig. 5 A compare in TTFAF and TBA among three NMA schemes. Scheme in [4] is a scheme proposed for Galileo with 120 bps data rate. Scheme [7] is a scheme proposed for BeiDou system with 50 bps data rate

$$\overline{TBA} = \frac{T_b L_f}{(1 - BER)^{L_f}} \tag{4.2}$$

Here L_f is length of the navigation message involved in one authentication fix, T_b is interval of navigation message bit, BER is bit error rate of navigation message.

A performance compare in efficiency between legacy NMA scheme integrated in satellite signal [4, 7] and the proposed NMA scheme assisted by GBAS is shown in Fig. 5. The proposed NMA scheme effectively reduce both TTFAF and TBA for the authentication.

In TTFAF aspect, the proposed scheme maintains a similar performance level as the scheme proposed in [4], which is a scheme with high efficiency in the 120 bps Galileo system. In TBA aspect, the proposed scheme is better than other twos schemes with the fastest authentication recovery.

5 Conclusion

This paper proposed an NMA scheme assisted by GBAS. Receivers can ensure the integrity of both navigation message and GBAS message via the proposed message type of GBAS broadcasting. The proposed scheme has an advantage in efficiency and authentication delay compared with legacy schemes integrated into satellite signal while has an equally high security level as other schemes.

Acknowledgements This work is supported by National Science Foundation of China (61601485).

References

1. Anonymous (2001) Vulnerability assessment of the transportation infrastructure relying on the global positioning system. John A. Volpe National Transportation Systems Center, U.S
2. Wullems C, Pozzobon O, Kubik K (2005) Signal authentication and integrity schemes for next generation global navigation satellite systems. In: Proceedings of the European navigation conference
3. Wesson KD, Rothlisberger MP, Humphreys TE (2011) A proposed navigation message authentication implementation for civil GPS anti-spoofing. In: Proceedings of the 24th international technical meeting of the satellite division of the institute of navigation (ION GNSS 2011), pp 3129–3140
4. Curran JT, Paonni M, Bishop J (2014) Securing the open-service: a candidate navigation message authentication scheme for Galileo E1 OS. In: European navigation conference ENC 2014, Rotterdam
5. Kerns AJ, Wessons K, Humphreys T (2014) A blueprint for civil GPS navigation message authentication. In: Proceedings of IEEE/ION PLANS 2014, Monterey, CA, pp 262–269
6. Hernandez IF, Rijmen V, Granados GS et al (2016) A navigation message authentication proposal for the Galileo open service. Navig J Inst Navig 63:85–102
7. Yuan M, Lv Z, Chen H et al (2017) An implementation of navigation message authentication with reserved bits for civil BDS anti-spoofing. In: China satellite navigation conference (CSNC) 2017 proceedings, Vol 2, pp 69–80
8. Hernaandez IF, Rijmen V, Granados GS, et al (2014) Design drivers, solutions and robustness assessment of navigation message authentication for the Galileo open service. In: Proceedings of the 27th international technical meeting of the satellite division of the institute of navigation (ION GNSS 2014), pp 2810–2827
9. Braff R, Shively C (2005) A method of over bounding ground based augmentation system (GBAS) heavy tail error distributions. J Navig 58:83–103
10. Dautermann T, Felux M, Grosch A (2012) Approach service type D evaluation of the DLR GBAS testbed. GPS Solut 16:375–387
11. Ludwig T, Korn B, Geister R, et al (2011) Towards higher levels of automation in taxi guidance: using GBAS terminal area path (TAP) messages for transmitting taxi routes. In: 30th digital avionics systems conference, Vol 4, No. 5, pp 1–11
12. Margaria D, Motella B, Anghileri M, et al (2017) Signal structure-based authentication for civil GNSSs: recent solutions and perspectives. In: IEEE signal processing magazine, pp 27–37
13. Johnson D, Menezes AJ, Vanstone SA (2001) The elliptic curve digital signature algorithm (ECDSA), certicom corporation
14. Perrig A, Canetti R, Tygar JD, Song D (2002) The TESLA broadcast authentication protocol. CryptoBytes 5(2):2–13
15. Gueneysu T, Paar C, Pelzl J (2007) Attacking elliptic curve cryptosystems with special-purpose hardware, field programmable gate arrays, pp 207–215